124 Let n be a natural state variable. Is the following specification implementable?

(a) $n:= n-1$

(b) $n>0 \Rightarrow (n:= n-1)$

(c) **if** $n>0$ **then** $n:= n-1$ **else** ok **fi**

After trying the question, scroll down to the solution.

(a) $n:=n-1$

§ $\forall n: nat\cdot \exists n': nat\cdot n:=n-1$ — expand assignment

$=$ $\forall n: nat\cdot \exists n': nat\cdot n' = n-1$ — specialization

$\Longrightarrow$ $\exists n': nat\cdot n' = 0-1$ — arithmetic

$=$ $\exists n': nat\cdot n'=-1$

$=$ $\bot$

So no, $n:=n-1$ is not implementable. From the line

$\forall n: nat\cdot \exists n': nat\cdot n' = n-1$ — we can use an identity law

$=$ $\forall n: nat\cdot \exists n': nat\cdot n' = n-1 \land \top$ — but now we cannot use the one-point law to get

$\forall n: nat\cdot \exists n': nat\cdot \top$ — because the one-point law requires $n-1: nat$

(b) $n>0 \Rightarrow (n:=n-1)$

§ $\forall n: nat\cdot \exists n': nat\cdot n>0 \Rightarrow (n:=n-1)$ — expand assignment

$=$ $\forall n: nat\cdot \exists n': nat\cdot n>0 \Rightarrow n' = n-1$ — distributive and identity

$=$ $\forall n: nat\cdot n>0 \Rightarrow \exists n': nat\cdot n' = n-1 \land \top$ — In the context $n>0$, $n-1: nat$. So we can use one-point.

$=$ $\forall n: nat\cdot n>0 \Rightarrow \top$ — base and identity

$=$ $\top$

So yes, $n>0 \Rightarrow (n:=n-1)$ is implementable.

(c) **if** $n>0$ **then** $n:=n-1$ **else** *ok* **fi**

§ $\forall n: nat\cdot \exists n': nat\cdot$ **if** $n>0$ **then** $n:=n-1$ **else** *ok* **fi** — expand assignment and *ok*

$=$ $\forall n: nat\cdot \exists n': nat\cdot$ **if** $n>0$ **then** $n' = n-1$ **else** $n'=n$ **fi** — case analysis

$=$ $\forall n: nat\cdot \exists n': nat\cdot (n>0 \land n' = n-1) \lor (n=0 \land n'=n)$ — splitting

$=$ $\forall n: nat\cdot (\exists n': nat\cdot n>0 \land n' = n-1) \lor (\exists n': nat\cdot n=0 \land n'=n)$ — In the context $n>0$, $n-1: nat$. And in the context $n=0$, $n: nat$. So we can apply one-point twice.

$=$ $\forall n: nat\cdot n>0 \lor n=0$

$=$ $\top$

So yes, **if** $n>0$ **then** $n:=n-1$ **else** *ok* **fi** is implementable.